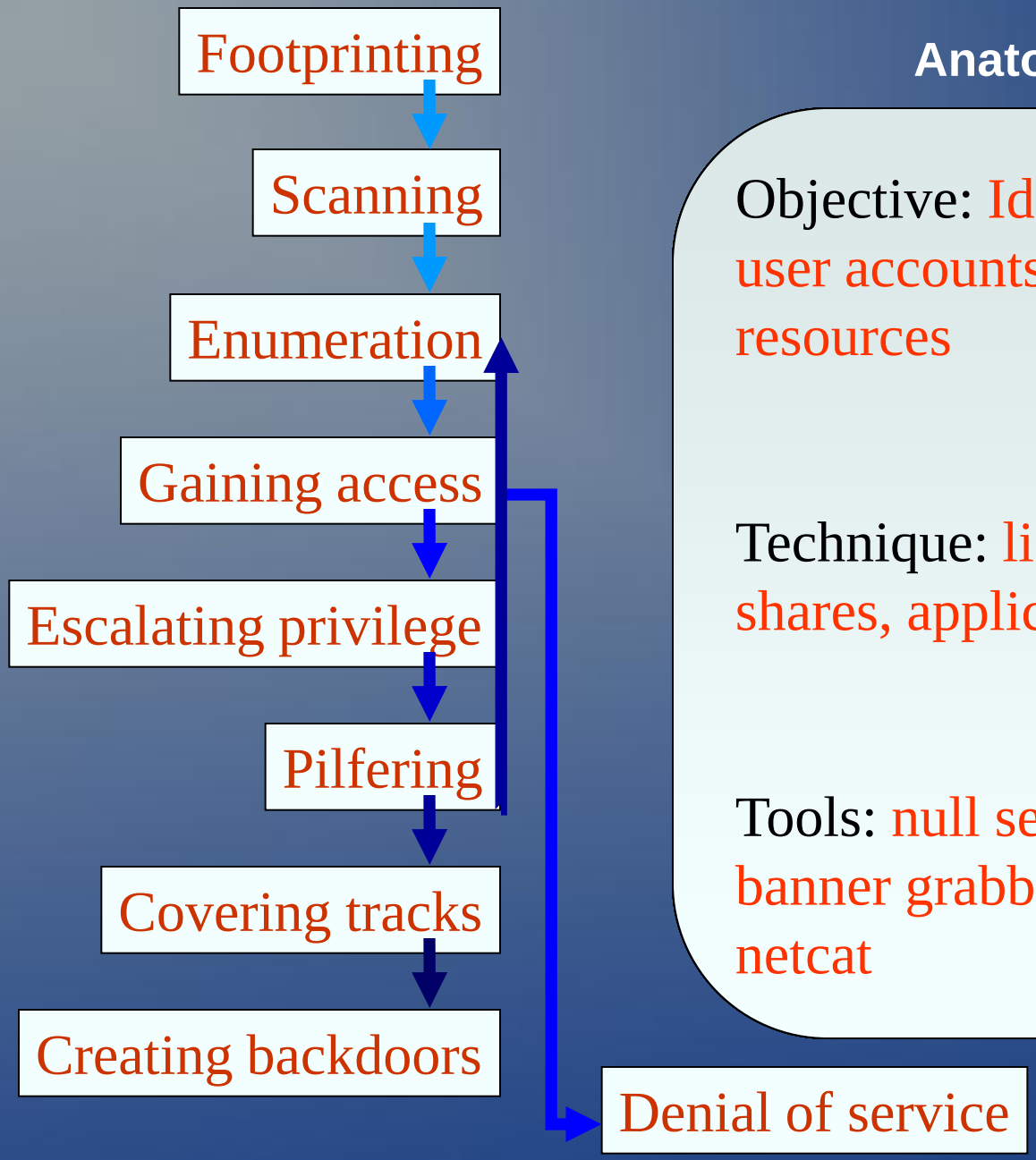
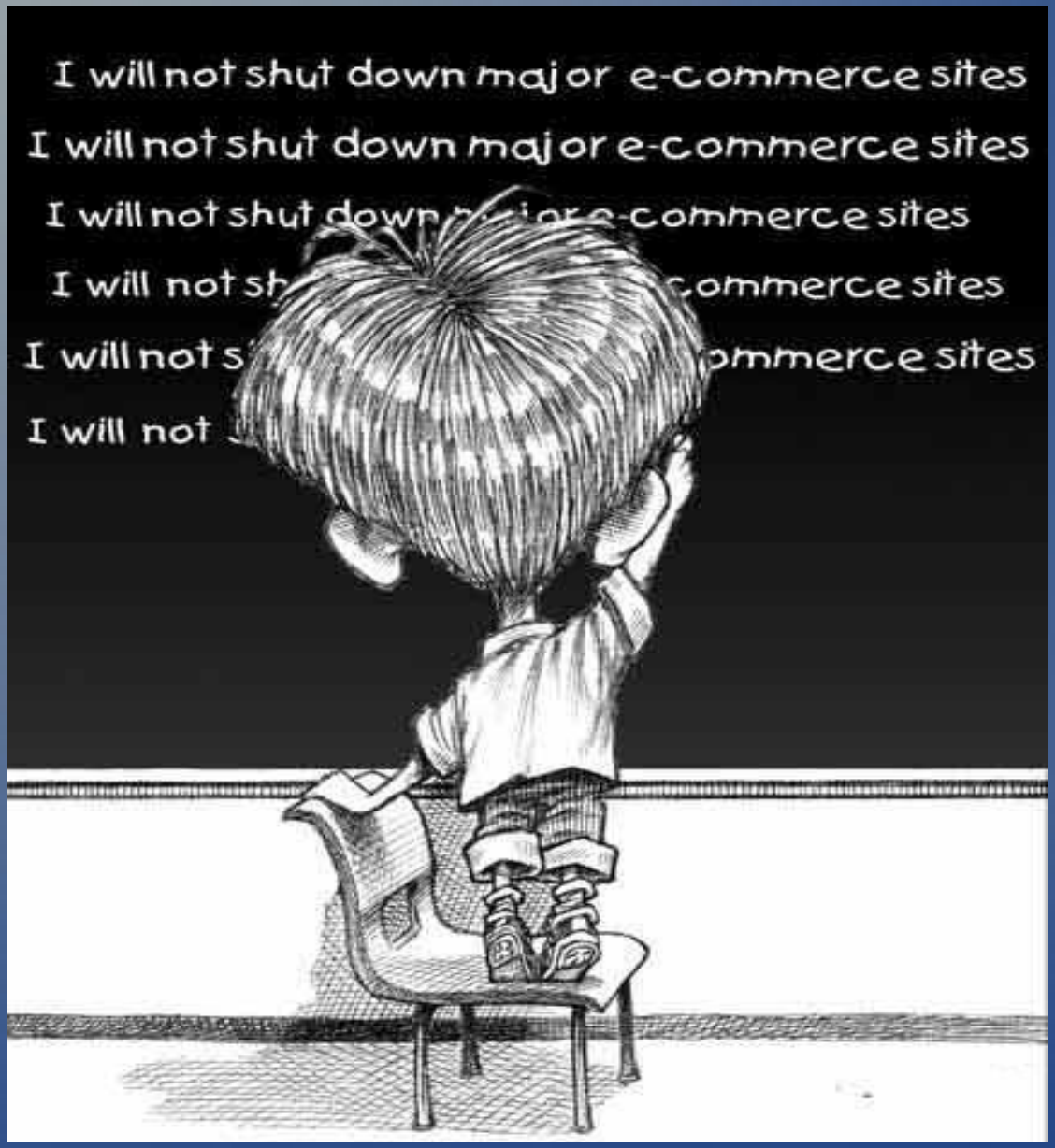


Anatomy of a hack

Objective: Identification of valid user accounts and poorly protected resources

Technique: list user accounts, file shares, applications

Tools: null sessions, showmount, banner grabbing with telnet or netcat



Web site – a perfect target

Web servers as targets

available to the entire world

24hrs online

HTTP (Hypertext Transfer Protocol) was not meant to be secure

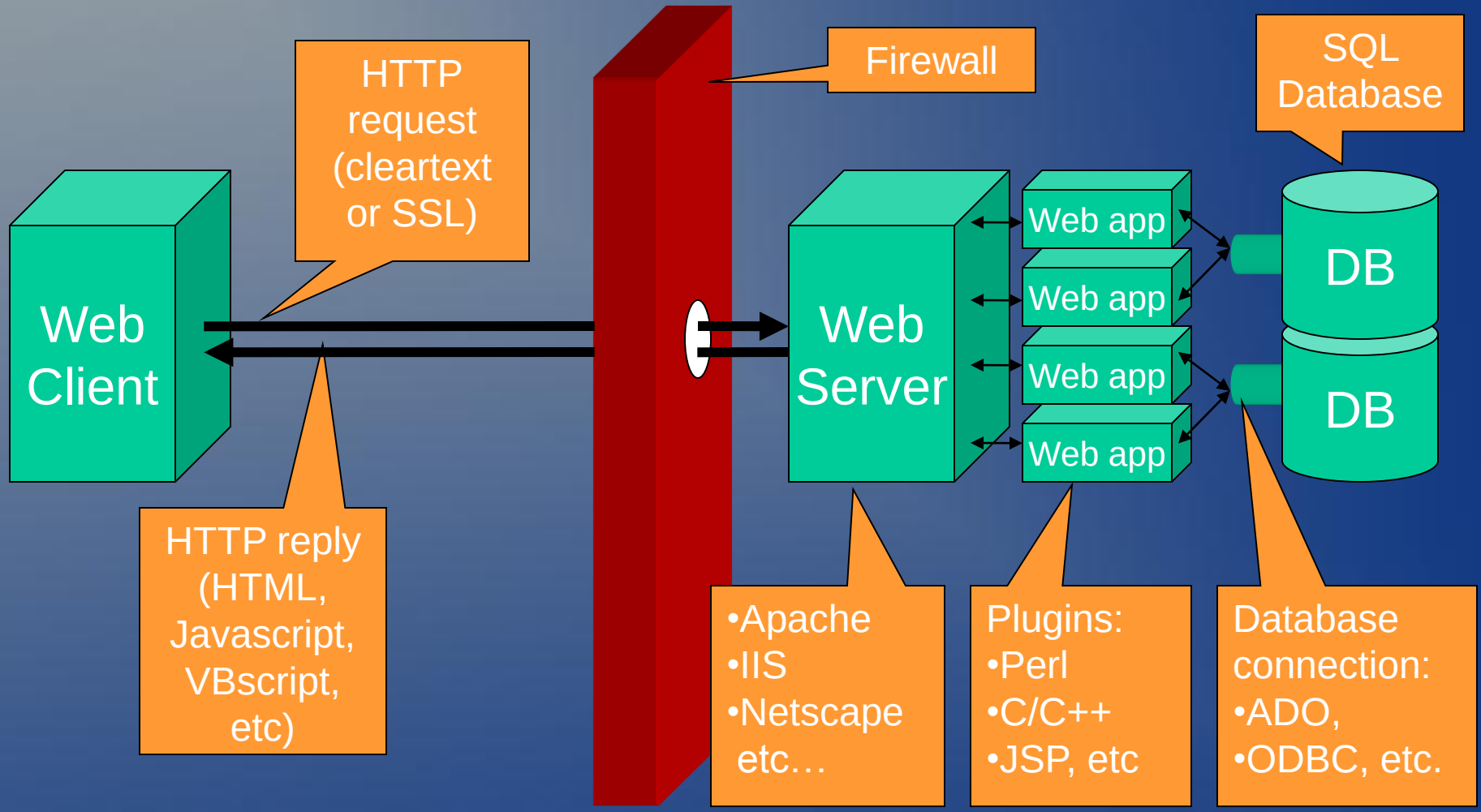
they can be pretty complex

no simple way to stop the attacker

the technology alone does not help you

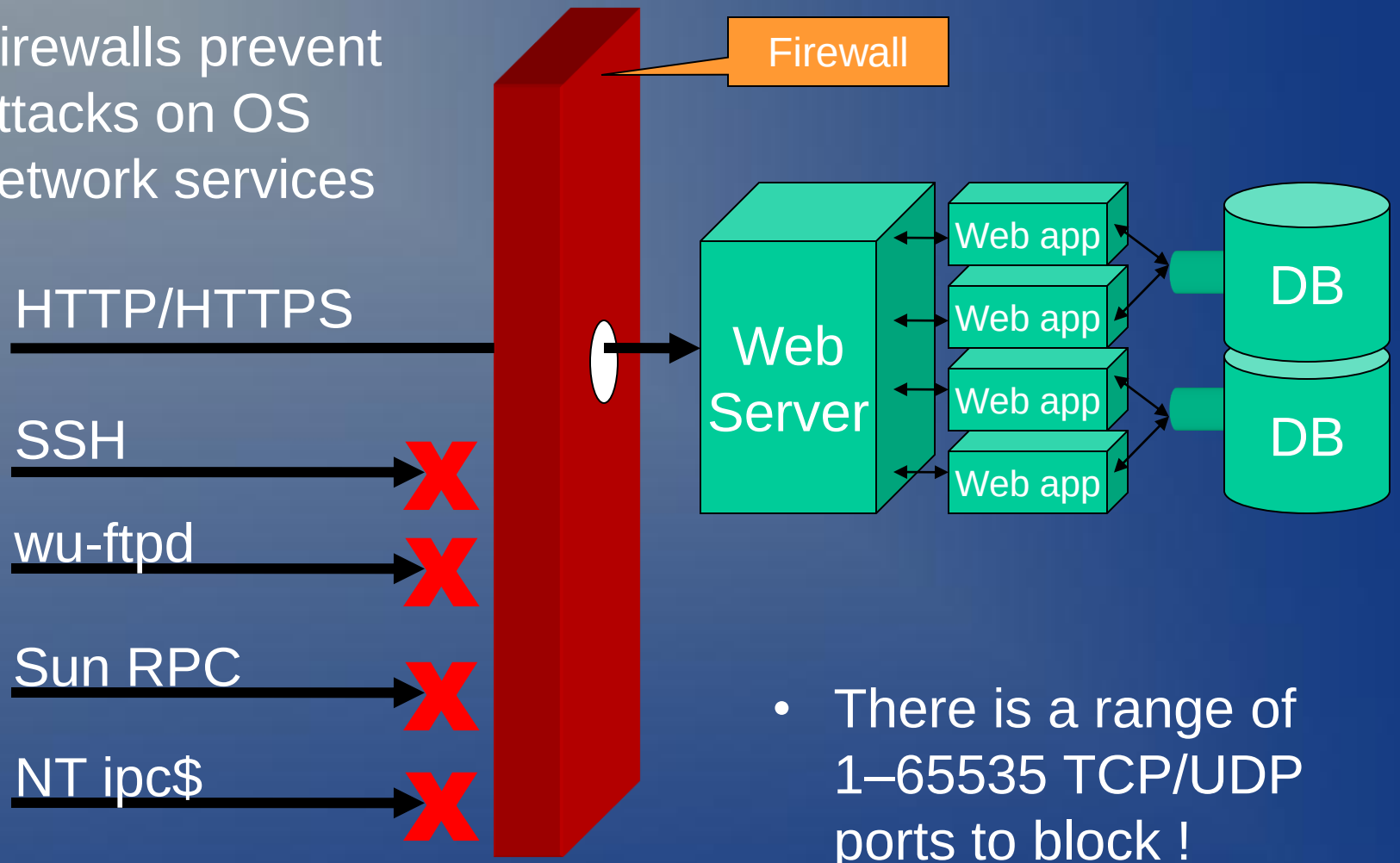
... the attacker simply has too many advantages and choices for attacks

a typical web server



Utility of firewalls

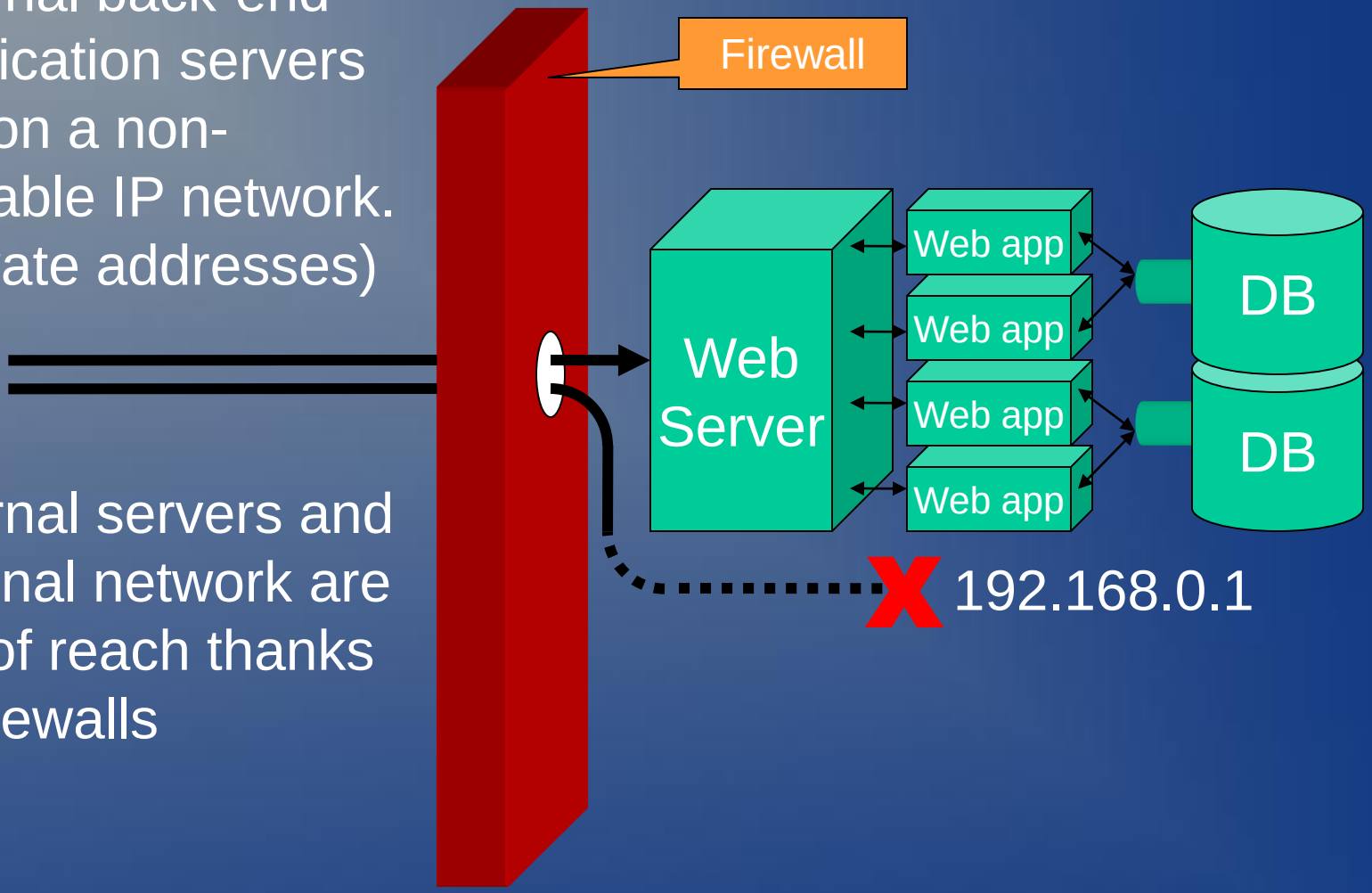
- Firewalls prevent attacks on OS network services



- There is a range of 1–65535 TCP/UDP ports to block !

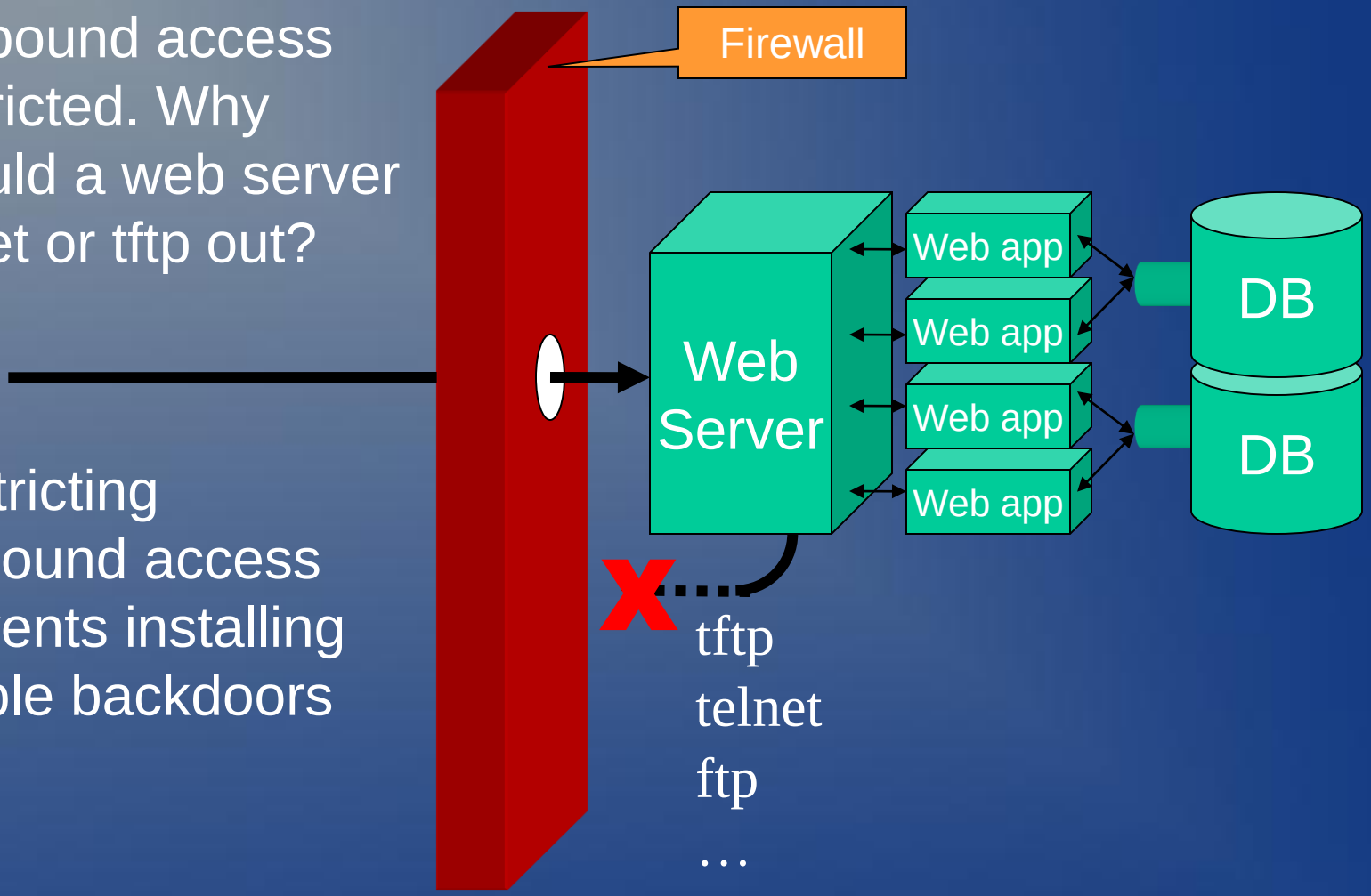
Utility of firewalls

- Internal back-end application servers are on a non-routable IP network. (private addresses)
- Internal servers and internal network are out of reach thanks to firewalls



Utility of firewalls

- Outbound access restricted. Why should a web server telnet or tftp out?
- Restricting outbound access prevents installing simple backdoors



Futility of firewalls

- E-commerce and Web hacking is not prevented
- Web traffic (HTTP/HTTPS) is the most commonly allowed of protocols through Internet firewalls
- Why fight the wall when you've got an open door?
- HTTP is normally perceived as "friendly" traffic and was not meant to be secure.
- Content/Application based attacks are still perceived as rare.

Web hacker’s toolbox

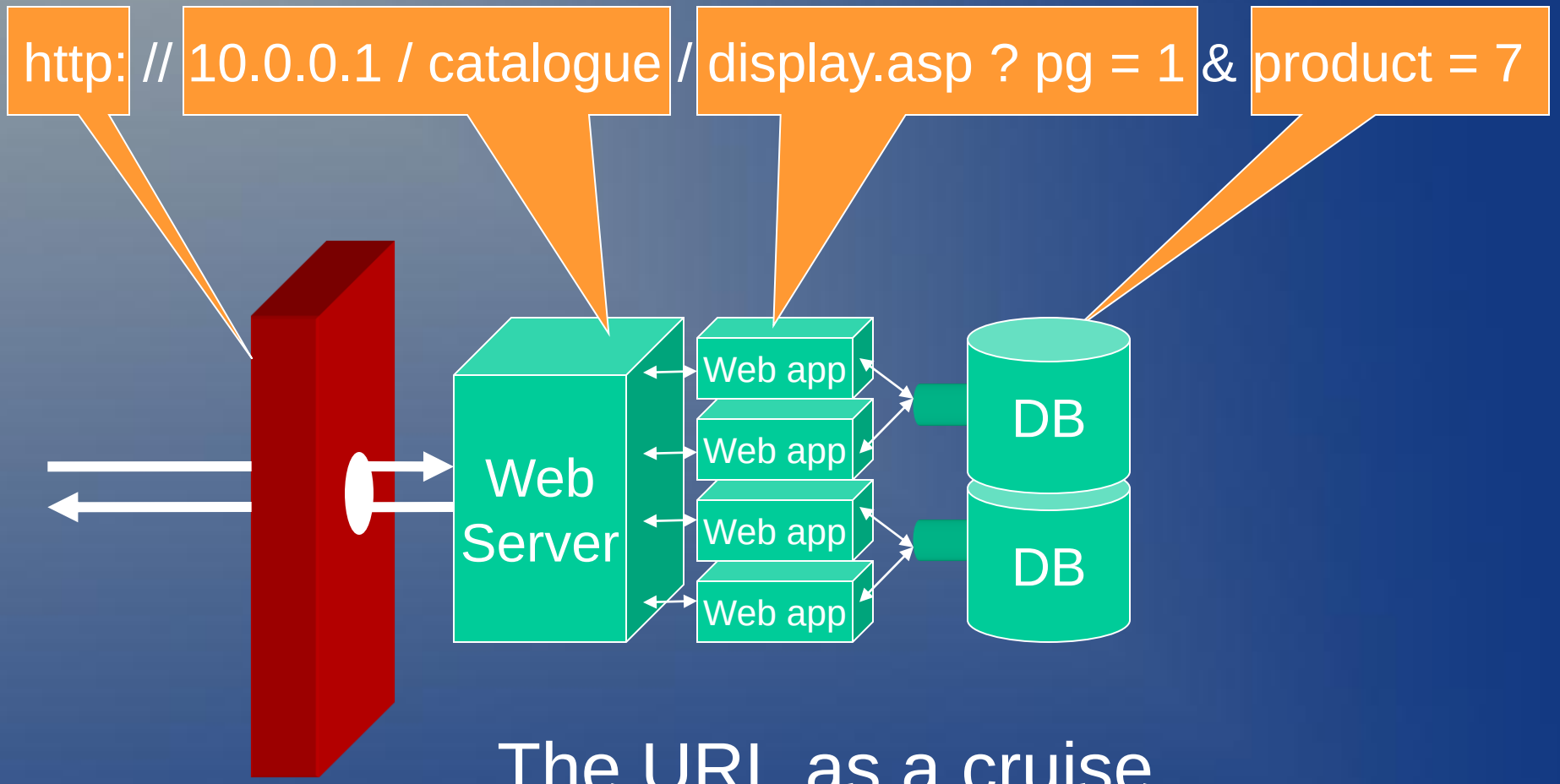
a web browser,

an Internet connection,

… and clear mind

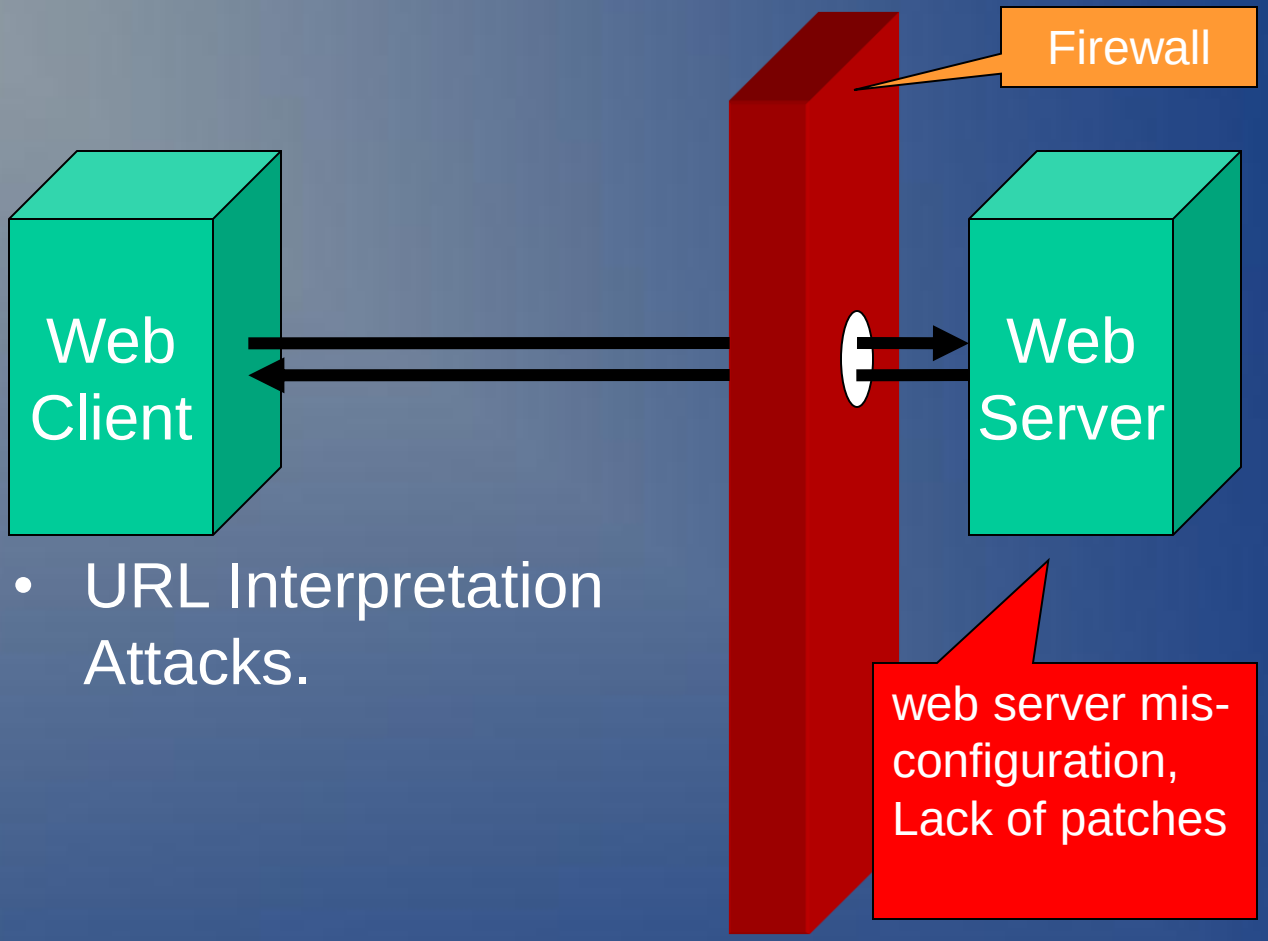
Could there be anything easier?

Why fight the wall?



The URL as a cruise missile!

Firewalls cannot prevent

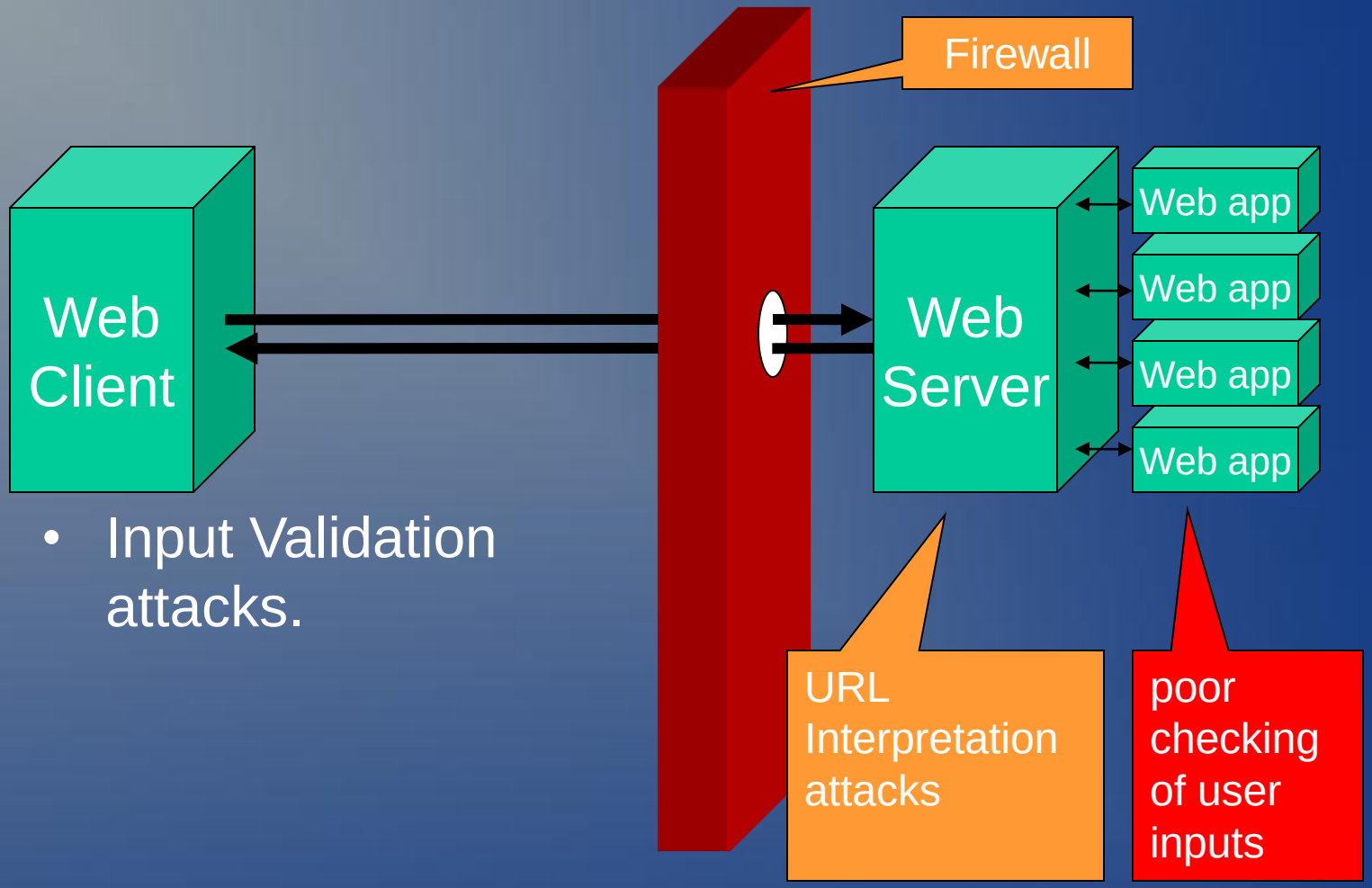


- URL Interpretation Attacks.

http://www.victim.com/scripts/..%%35c..%%35cwinnt/system32/cmd.exe?/c+dir+c:\

Microsoft IIS Unicode exploit

Firewalls cannot prevent

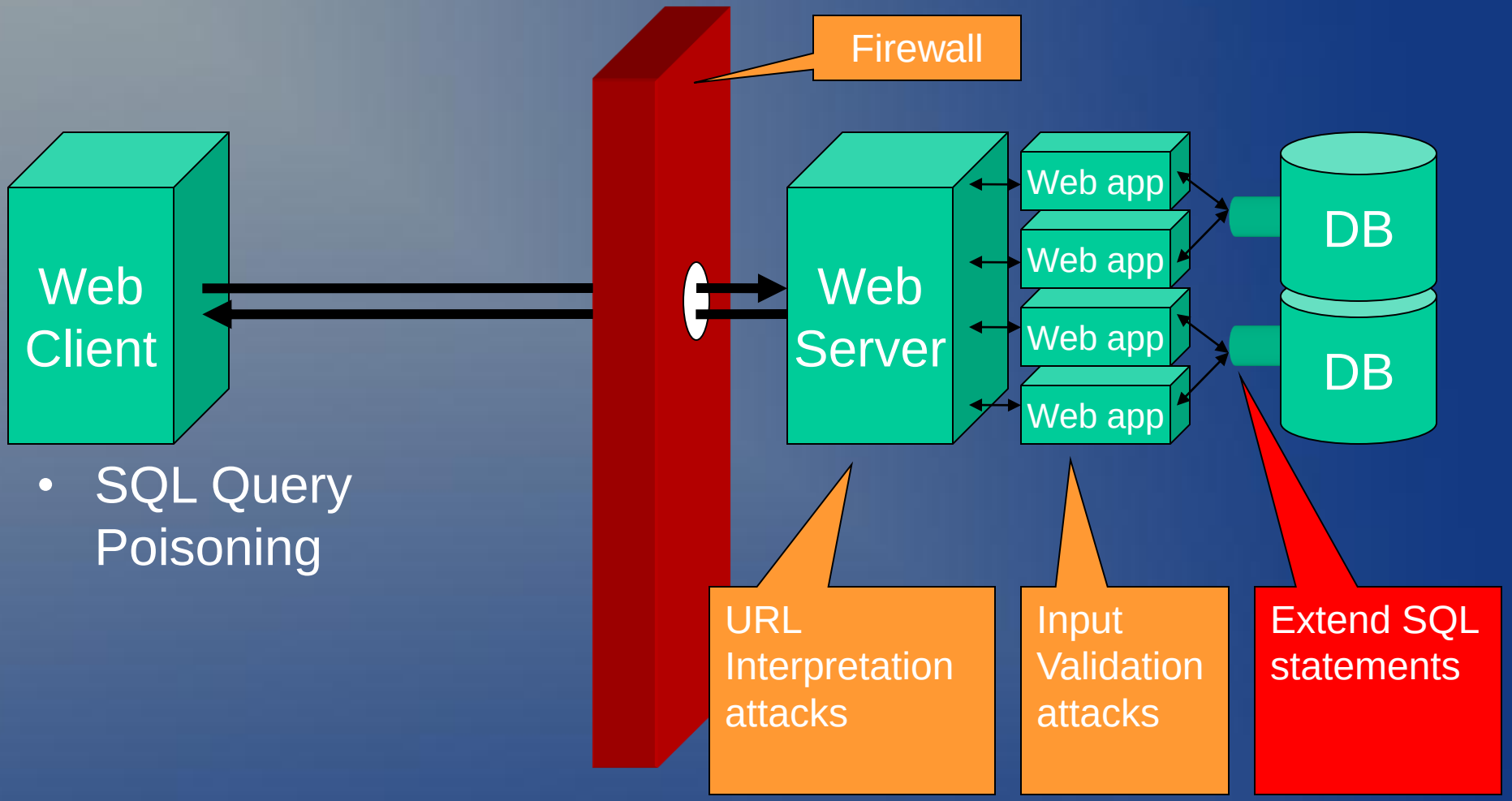


- Input Validation attacks.

user: ‘or’a‘=’a pass: ‘or’a‘=’a

Hacking with Google

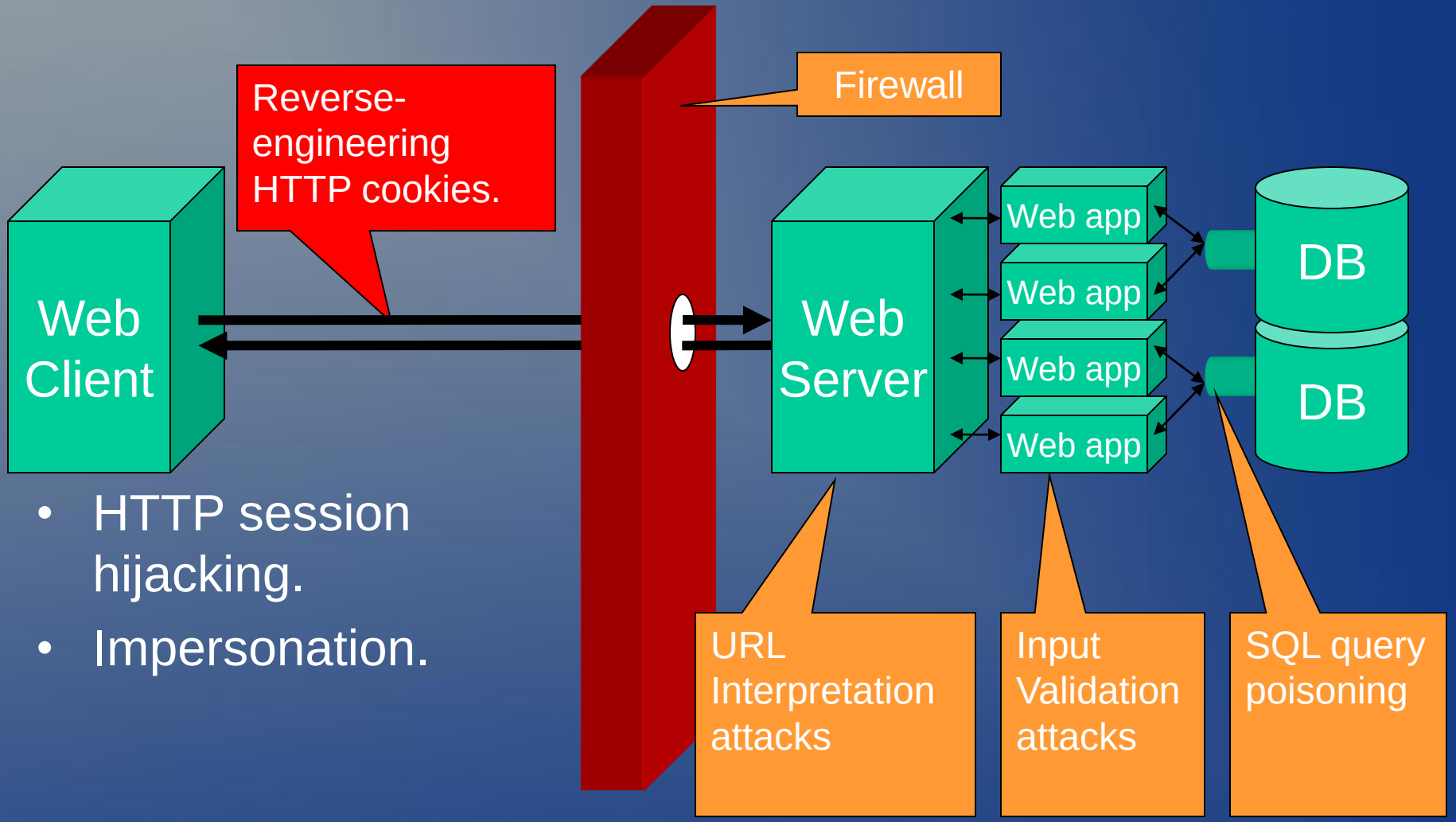
Firewalls cannot prevent



- SQL Query Poisoning

http://www.victim.com/script?0';EXEC+master..xp_cmdshell(cmd.exe+/c);--

Firewalls cannot prevent



- HTTP session hijacking.
- Impersonation.

What good is SSL for?

Secure Sockets Layer (SSL)

SSL is only meant to authenticate the server for a user and to do point-to-point encryption so that no one can tap into the traffic

1. It does nothing to prevent direct attacks
2. SSL session could be still tapped into or hijacked (e.g. Man-In-The-Middle (MITM) attack)

Hijacking SSL session

Tools are easily available:

Netcat (freeware)

http://www.atstake.com/research/tools/network_utilities/

+

OpenSSL (freeware)

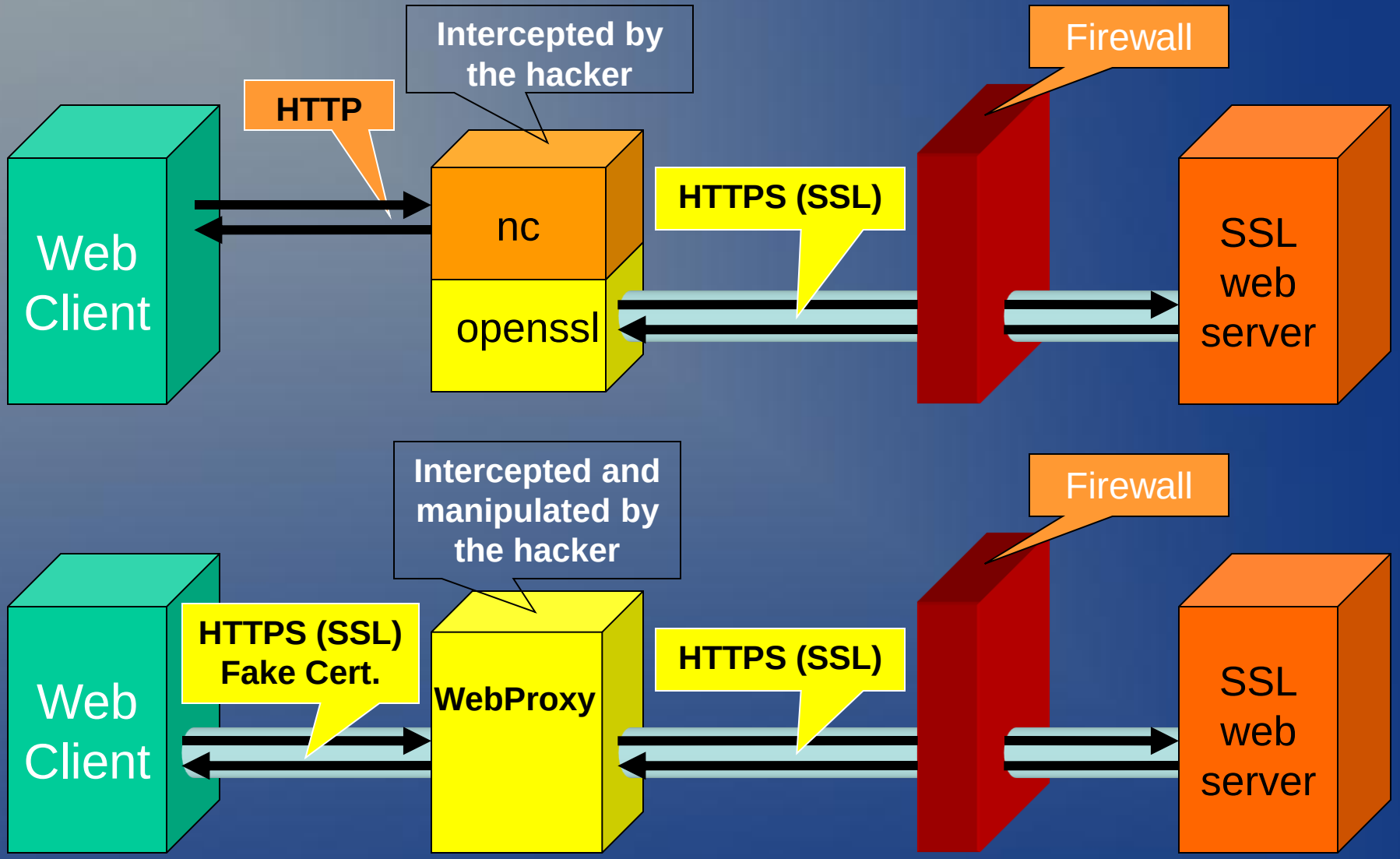
http://www.openssl.org/

or

@Stake WebProxy (no longer freeware)

http://www.atstake.com/webproxy/

Web SSL MITM


Intercepted by the hacker
HTTP
Firewall
Web Client
nc
openssl
HTTPS (SSL)
SSL web server
Intercepted and manipulated by the hacker
Firewall
HTTPS (SSL) Fake Cert.
Web Client
WebProxy
HTTPS (SSL)
SSL web server

these were just a few examples…

http://www.owasp.org/ **Top 10 web application security issues:**

http://prdownloads.sourceforge.net/owasp/OWASPWebApplicationSecurityTopTen-Version1.pdf?download

1. Unvalidated Parameters
2. Broken Access Control
3. Broken Account and Session Management
4. Cross-Site Scripting (XSS) Flaws
5. Buffer Overflows
6. Command Injection Flaws
7. Error Handling Problems
8. Insecure Use of Cryptography
9. Remote Administration Flaws

Penetration testing gives what?

- Outsiders look at your security (weaknesses)
- Independent assurance from experts
- Methodical review of EVERY aspect
- Verifies the job of your IT staff or/and application service provides (ASP)

Makes you aware of your weaknesses before someone strikes!

Security testing terms

Black-box

any testing that is done without prior knowledge, blindly but not randomly.

White-box

any testing completed with privileged knowledge, i.e. having the source code for a program while testing.

Passive

data collection by not probing or attaching to non-public parts of a system or network.

Invasive

trespassing by probing or attaching to non-public parts of a system or network.